Policy di Sicurezza per i Servizi di Pagamento via *Internet*

Abstract	Policy che definisce i ruoli e le responsabilità, i processi ed i presidi posti in essere dalla Banca riguardo alla valutazione, al controllo ed alla mitigazione dei rischi derivanti dalla sicurezza dei pagamenti via *Internet*
Tipologia	Policy
Autore	Debora Terenziani (Responsabile Ufficio IT)
Responsabile del documento (*)	Debora Terenziani (Responsabile Ufficio IT)
Uso	Interno
Organo e data di approvazione	CDA – 22 SETTEMBRE 2016
Versioni precedenti	NA
Variazioni di rilievo	NA
Localizzazione	Logical doc – Sito *Internet* Banca
Visto di conformità	Validazione di conformità ricevuta in data 21/09/2016

(*) Il Responsabile del documento provvede alla sua pubblicazione, nonché al suo costante aggiornamento normativo ed operativo

SOMMARIO

1. PREMESSA

Il presente documento riporta la Policy esistente in Banca Privata Leasing in tema di sicurezza per i servizi di pagamento via *Internet*.

In particolare secondo quanto enunciato dalla disciplina normativa vigente (16° aggiornamento della Circ.285/2013 di Banca d'Italia, parte Prima, Titolo IV, Capitolo 4 "Il sistema informativo") la Banca, in quanto prestatrice di servizi di pagamento tramite canale *Internet* alla clientela, si attiene agli "Orientamenti finali sulla sicurezza dei pagamenti via *Internet*" dell'EBA del 19 dicembre 2014. Si rimanda a tali normative per approfondimenti regolamentari sul tema e per l'elenco delle definizioni richiamate dalla disciplina vigente.

In linea con l'impostazione generale della disciplina in materia di controlli interni e gestione dei rischi e fermi restando i casi di obblighi specifici, Banca Privata Leasing applica le disposizioni contenute negli Orientamenti secondo il principio di proporzionalità, cioè tenuto conto della dimensione e della complessità operativa, della natura dell'attività svolta e della tipologia di servizi prestati.

Inoltre, BPL si avvale dell'esternalizzazione dei servizi ICT presso CSE con servizi trasversali come il *facility management*, la gestione degli apparati hardware, lo sviluppo e la gestione del parco applicativo dei processi bancari (*application management*): in tale contesto, si inserisce il canale *online* relativo ai servizi di *Internet Banking* per la clientela ed i relativi presidi in tema di sicurezza dei pagamenti via *Internet*.

Nei prossimi capitoli verranno richiamati sinteticamente, secondo i macro-ambiti indicati di seguito, i principi delineati negli Orientamenti accompagnati da una descrizione dei ruoli e delle responsabilità, dei processi e dei presidi posti in essere dalla Banca in tema di valutazione, controllo e mitigazione dei rischi derivanti dall'attività di prestatrice di servizi di pagamento via *Internet*:

- controllo generale e ambiente di sicurezza;
- misure specifiche di controllo e di sicurezza per i pagamenti via *Internet*;
- sensibilizzazione, educazione e comunicazione riguardanti il cliente.

All'interno della presente Policy non verranno richiamati gli specifici Orientamenti relativi all'operatività non significativa per Banca Privata Leasing (es: *aquiring* per esercenti *online, virtual cards, etc..)*.

2. CONTROLLO GENERALE E AMBIENTE DI SICUREZZA

2.1 Governance (pto 1 Eba)

La presente policy di sicurezza per i servizi di pagamento via *Internet* è stata approvata dall'organo di supervisione strategica e di gestione della Banca, ai sensi della normativa di riferimento ed in coerenza con il modello di *governance* adottato da Banca Privata Leasing.

Tale documento viene riesaminato periodicamente alla luce dell'evoluzione del relativo rischio ed in conseguenza di mutamenti significativi alle linee guide strategiche ed operative della Banca e/o all'infrastruttura tecnologica attuale.

Le politiche gestionali di Banca Privata Leasing sono costantemente ispirate al rispetto della sana e prudente gestione di tutti i rischi connessi alla stessa, ivi compreso il rischio informatico, che risulta essere rilevante in particolare per la significativa quota di raccolta da clientela acquisita tramite il canale *Internet*.

L'obiettivo definito dall'organo di supervisione strategica e di gestione della Banca è quello di minimizzare quanto più questo rischio e specificatamente di valutare, controllare e mitigare il relativo rischio di mancata sicurezza dei pagamenti via *Internet*, dato che oltre al puro rischio operativo ed informatico potrebbe avere importanti ripercussioni in termini di rischio reputazionale: pertanto il Consiglio di Amministrazione considera una propensione al rischio informatico (e al tema specifico della sicurezza dei pagamenti via *Internet*) medio-basso con l'obiettivo di mitigarlo quanto più attraverso un adeguato presidio e controllo delle risorse tecnologiche, delle procedure informatiche e dei processi coinvolti (anche esternalizzate presso l'*outsourcer* CSE).

Le funzioni della Banca coinvolte sono rappresentate da:

- Consiglio di Amministrazione: in quanto organo con funzione di supervisione strategica e di gestione della Banca, definisce le linee guida, gli obiettivi di rischio e la propensione al rischio della Banca, compreso il rischio informatico. In particolare, come da normativa vigente:
  - approva le strategie di sviluppo del sistema informativo;
  - approva la *policy* di sicurezza informatica;
  - è informato con cadenza almeno annuale circa l'adeguatezza dei servizi erogati e il supporto di tali servizi all'evoluzione dell'operatività aziendale, in rapporto ai costi sostenuti;

- è informato tempestivamente in caso di gravi problemi per l'attività aziendale derivanti da incidenti e malfunzionamenti del sistema informativo ed in materia di sicurezza informatica;
- approva e definisce il quadro di riferimento organizzativo, metodologico e procedurale per l'analisi del rischio informatico;
- approva la propensione al rischio informatico e viene informato con cadenza almeno annuale sulla situazione del rischio informatico rispetto alla propensione al rischio definita;
- definisce la struttura organizzativa della funzione ICT e l'assetto organizzativo, metodologico e procedurale per il processo di analisi del rischio informatico;
- approva gli *standard* di *data governance*, le procedure di gestione dei cambiamenti e degli incidenti in raccordo con le procedure del fornitore di servizi, il piano operativo delle iniziative informatiche, la valutazione del rischio delle componenti critiche e la relazione sull'adeguatezza e costi dei servizi ICT;
- valuta le prestazioni della funzione ICT rispetto alle strategie e agli obiettivi fissati, in termini di rapporto costi / benefici;
- monitora il regolare svolgimento dei processi di gestione e di controllo dei servizi ICT;
- assume decisioni tempestive in merito a gravi incidenti di sicurezza informatica.

- IT: svolge la funzione di sicurezza informatica ed è deputata allo svolgimento dei compiti specialistici in materia di sicurezza delle risorse ICT. In particolare:
  - segue la redazione e l'aggiornamento delle *policy* di sicurezza e delle istruzioni operative;
  - assicura la coerenza dei presidi di sicurezza con le *policy* approvate;
  - partecipa alla progettazione, realizzazione e manutenzione dei presidi di sicurezza dei *data center*;
  - partecipa alla valutazione del rischio potenziale nonché all'individuazione dei presidi di sicurezza nell'ambito del processo di analisi del rischio informatico;
  - assicura il monitoraggio nel continuo delle minacce applicabili alle diverse risorse informatiche;
  - segue lo svolgimento dei test di sicurezza prima dell'avvio in produzione di un sistema nuovo o modificato.

- Risk Management: basandosi su flussi informativi in merito all'evoluzione del rischio informatico e sul monitoraggio di efficacia delle misure di protezione delle risorse ICT, svolge il compito di controllo di tali rischi. Le valutazioni effettuate, riportate all'organo di supervisione strategica e di gestione e alla vigilanza esterna, sono documentate e riviste in rapporto ai risultati del monitoraggio e comunque almeno una volta all'anno.

- Compliance: verifica il rispetto dei regolamenti interni e delle normative esterne in tema di ICT (ICT *Compliance*) garantendo tra l'altro l'assistenza su aspetti tecnici in caso di questioni legali relative al trattamento dei dati personali, la coerenza degli assetti organizzativi alle normative esterne, per le parti relative al sistema informativo e l'analisi di conformità dei contratti di *outsourcing* e con fornitori (inclusi i contratti infra-gruppo).

- Internal Audit: assolve ai propri compiti di *assurance* attinenti al sistema informativo aziendale (ICT *Audit*), eventualmente anche mediante il ricorso a risorse specialistiche esterne indipendenti.

- Antiriclaggio: nell'ambito dei controlli svolti dalla funzione viene garantito che il processo di adeguata verifica venga attuato prima dell'apertura del rapporto contrattuale per tutta la clientela e quindi prima che il cliente sia autorizzato ad accedere ai servizi.

- Canale *Online*: cura la distribuzione alla clientela dei prodotti e dei servizi bancari distribuibili tramite il canale *online* (c/c, carte di debito/credito, domiciliazione di utenze e deleghe, servizi telematici, etc.) ed in particolare propone, nel rispetto di quanto previsto dalla normativa in materia di vendite a distanza, prodotti e servizi alla clientela e supporta ed assiste la clientela nella fase di pre e post vendita (es: processo di sblocco delle credenziali di accesso alla procedura di *Home Banking*).

- Organizzazione: si occupa di gestire la struttura organizzativa mediante la definizione dei processi interni ed il coordinamento dell'emanazione della regolamentazione interna, garantendo la fruibilità delle strutture informatiche e logistiche di supporto all'attività della Banca.

In tale contesto, riveste un ruolo fondamentale l'*outsourcer* informatico CSE che fornisce la piattaforma di *Internet Banking* e che ha definito una propria policy di sicurezza per gli *Internet Payment* anch'essa approvata dal relativo Consiglio di Amministrazione.

2.2 Valutazione dei Rischi (pto 2 Eba)

Banca Privata Leasing svolge e documenta valutazioni dei rischi approfondite per i pagamenti via *Internet* e i servizi connessi, tiene conto dei risultati del monitoraggio costante delle minacce alla sicurezza dei servizi di pagamento via *Internet* che offre, tenendo in considerazione le soluzioni tecnologiche utilizzate, i servizi affidati a operatori esterni, l'ambiente tecnico dei Clienti come pure i risultati del processo di monitoraggio degli incidenti riguardanti la sicurezza e l'esigenza di proteggere e tutelare i dati sensibili relativi ai pagamenti.

La Banca stabilisce se e quanto possono rivelarsi necessarie modifiche alle misure di sicurezza esistenti, alle tecnologie utilizzate e alle procedure o ai servizi resi, tenendo in considerazione il tempo necessario per mettere in atto le modifiche e adottare i provvedimenti provvisori necessari per ridurre al minimo gli incidenti di sicurezza e le frodi, nonché i potenziali effetti pregiudizievoli.

Una revisione degli scenari di rischio e delle misure di sicurezza esistenti viene effettuata almeno una volta all'anno e viene sottoposta all'approvazione del Consiglio di Amministrazione ed in particolare in caso di incidenti gravi, prima di un cambiamento importante delle infrastrutture o delle procedure o quando nuove minacce sono individuate attraverso l'attività di monitoraggio dei rischi.

In tale contesto:

- l'*outsourcer* informatico (CSE) sviluppa con frequenza annuale un'analisi del rischio informatico che comprende tutti i servizi tecnologici offerti compresi quelli correlati ai sistemi di pagamento *online* forniti alle Banche del consorzio. Inoltre CSE:
  - svolge specifiche valutazioni di impatto anche sulla valutazione dei rischi sia nell'ambito del proprio processo di gestione degli incidenti che nell'ambito del proprio processo di *change management*;
  - nell'ambito della propria valutazione dei rischi considera l'esigenza di proteggere e tutelare i dati sensibili relativi ai pagamenti (es: i numeri delle carte di credito non sono esposti in chiaro);
  - prevede all'interno della propria procedura di gestione degli incidenti l'attivazione eventuale del processo di valutazione dei rischi.

- il responsabile Risk Management, in collaborazione con l'Ufficio IT, monitora trimestralmente all'interno del documento Risk Appetite Framework (RAF), condiviso ed approvato dal Consiglio di Amministrazione ed inviato a Banca d'Italia, il livello del rischio informatico della Banca e specificatamente per quel che riguarda la sicurezza dei pagamenti via *Internet* controlla l'evoluzione, la frequenza\rilevanza degli incidenti\anomalie informatiche ed espone qualitativamente un commento sul relativo rischio residuo e sullo scenario di rischio analizzato.

- il responsabile dell'Ufficio IT informa con cadenza almeno annuale, ovvero con tempestività in caso di episodi negativi significativi rilevati, il Consiglio di Amministrazione relativamente alla situazione della sicurezza informatica della Banca.

L'Ufficio IT ed il responsabile Risk Management, a seguito dei relativi controlli, possono proporre al Consiglio di Amministrazione eventuali revisioni ed implementazioni al sistema di sicurezza di Banca Privata Leasing: di volta in volta, a seconda della rilevanza degli accadimenti negativi, si valuterà se richiedere modifiche\aggiornamenti agli applicativi dell'*outsourcer informatico* CSE e/o cambiamenti nel processo di controllo e/o di intraprendere campagne di comunicazione e sensibilizzazione specifiche alla clientela.

2.3 Monitoraggio e segnalazione degli incidenti (pto 3 Eba)

Banca Privata Leasing ha strutturato un processo utile a monitorare, gestire e seguire gli incidenti relativi alla sicurezza e i reclami dei Clienti in materia di sicurezza, e riferire tali incidenti all'organo di supervisione strategica e di gestione.

In caso di gravi incidenti relativi alla sicurezza dei pagamenti con riferimento ai servizi di pagamento prestati, la Banca si avvale di una procedura di comunicazione immediata alle autorità competenti e di una procedura per la cooperazione con i competenti organismi di esecuzione della legge.

In tale contesto:

- l'*outsourcer* informatico (CSE) dispone di una propria procedura per la gestione degli incidenti;
- la Banca ha strutturato un processo di monitoraggio e di gestione degli incidenti relativi alla sicurezza e ai reclami dei Clienti in materia di sicurezza, come delineato nei due paragrafi che seguono. Inoltre Banca Privata Leasing partecipa attivamente alla cooperazione sui temi di sicurezza informatica, tramite l'adesione al gruppo di presidio *Internet* promosso da AbiLab.

2.3.1 Processo di monitoraggio e gestione degli incidenti

Banca Privata Leasing ha strutturato il seguente processo operativo di gestione e monitoraggio degli incidenti in ambito di sicurezza informatica distinto a seconda del soggetto che segnala l'evento anomalo.

2.3.1.1 Outsourcer Informatico CSE:

- CSE segnala l'evento anomalo a Banca Privata Leasing (l'ufficio Organizzazione segnala tempestivamente la casistica alla Filiale, responsabile del Canale *online*, all'Ufficio IT e al responsabile Risk Management);
- Se il bonifico deve essere ancora essere autorizzato, la Filiale contatta il cliente per un confronto al fine di capire se il pagamento è legittimo e quindi l'operazione potrà:
    - essere autorizzata, se il cliente conferma che il pagamento è legittimo;
    - essere bloccata definitivamente → in tal caso verrà effettuata una comunicazione formale al cliente via mail.
- Se il bonifico è già stato autorizzato, ma non ancora spedito, la Filiale contatta il cliente per un confronto al fine di capire se il pagamento è legittimo e quindi l'operazione potrà:
    - essere autorizzata, se il cliente conferma che il pagamento è legittimo;
    - essere cancellata → in tal caso verrà effettuata una comunicazione formale al cliente via mail.
- Se il bonifico è già stato autorizzato e spedito e quindi l'operazione è già eseguita → in tal caso verrà effettuata comunque una comunicazione formale al cliente via mail, indicando che è stata notata un'anomalia sulla stessa e per richiederne un commento.

2.3.1.2 Banca Privata Leasing:

- Se il bonifico deve essere ancora essere autorizzato, la Filiale contatta il cliente per un confronto al fine di capire se il pagamento è legittimo e quindi l'operazione potrà:
    - essere autorizzata, se il cliente conferma che il pagamento è legittimo;
    - essere bloccata definitivamente → in tal caso verrà effettuata una comunicazione formale al cliente via mail.

- Se il bonifico è già stato autorizzato, ma non ancora spedito, la Filiale contatta il cliente per un confronto al fine di capire se il pagamento è legittimo e quindi l'operazione potrà:
    - essere autorizzata, se il cliente conferma che il pagamento è legittimo;
    - essere cancellata → in tal caso verrà effettuata una comunicazione formale al cliente via mail.
- Se il bonifico è già stato autorizzato e spedito e quindi l'operazione è già eseguita → in tal caso verrà effettuata comunque una comunicazione formale al cliente via mail, indicando che è stata notata un'anomalia sulla stessa e per richiederne un commento.

2.3.1.3 Clientela

- Il cliente che vuole segnalare l'anomalia lo comunica alla Banca secondo i seguenti canali:
    - FILIALE (o TELEFONATA) – l'operazione verrà bloccata dalla Filiale (se non ancora eseguita) e verrà rilasciato al cliente (oppure inviato via mail) un documento attestante quanto emerso dalla sua segnalazione;
    - POSTA ELETTRONICA (indirizzo SICUREZZA@BANCAPRIVATALEASING.IT) - l'Ufficio IT, destinatario della mail, avvertirà la filiale che bloccherà l'operazione (se non ancora eseguita) ed invierà via mail al cliente un documento attestante quanto emerso dalla sua segnalazione;

In tutti i casi segnalati l'Ufficio IT ed il responsabile Risk Management vengono informati dalla Filiale e redigono uno specifico verbale per ogni casistica segnalata. Tali verbali vengono raccolti e monitorati all'interno di uno specifico registro tenuto a cura del responsabile Risk Management;

In caso di accadimenti negativi particolarmente gravi l'Ufficio IT e/o il responsabile Risk Management informano in maniera tempestiva le autorità competenti attraverso PEC (Poste Elettronica Certificata), il Consiglio di Amministrazione della Banca ed il gruppo di lavoro per la cooperazione AbiLab.

2.3.2 Processo di gestione dei reclami della clientela in materia di sicurezza

In caso di reclamo da parte della Clientela la gestione dello stesso avviene applicando lo "*standard* operativo" delineato dalla Banca per casi analoghi, ovvero come indicato all'interno del sito nella sezione "Trasparenza" – "Reclami" e come precisato in maniera dettagliata all'interno del relativo "Regolamento Reclami" presente nella stessa pagina *web* e consultabile liberamente.

2.4 Controllo e mitigazione dei rischi (pto 4 Eba)

L'*outsourcer* informatico nell'ambito delle proprie prassi e procedure operative (e l'infrastruttura del sistema informativo) rispetta i seguenti requisiti regolamentari:

- nella progettazione nello sviluppo e nel mantenimento dei servizi di pagamento via *Internet* viene garantita un'adeguata separazione dei compiti e dei ruoli negli ambienti della tecnologia dell'informazione (IT) (per esempio gli ambienti di sviluppo, di prova e di produzione) e alla corretta applicazione del principio del "privilegio minimo" quale base per una sana gestione delle identità e degli accessi;
- dispone di soluzioni di sicurezza adeguate per proteggere le reti, i siti web, i server e i collegamenti di comunicazione contro abusi o attacchi;
- disattiva nei server tutte le funzioni superflue al fine di proteggerli ('*hardening*') e di eliminare o ridurre le vulnerabilità delle applicazioni a rischio;
- l'accesso mediante le varie applicazioni ai dati e alle risorse necessarie viene ridotto al minimo indispensabile secondo il principio del "privilegio minimo";
- al fine di limitare l'uso di "falsi" siti web (che imitano i siti legittimi dei prestatori di servizi di pagamento), i siti web transazionali che offrono servizi di pagamento via *Internet* sono identificati mediante estesi certificati di convalida redatti a nome del prestatore di servizi di pagamento o con altri metodi di autenticazione equivalenti;
- si avvale di processi idonei per monitorare, tenere traccia (crea, conserva ed analizza adeguati registri e procedimenti di tracciabilità dei dati – piste di controllo) e limitare l'accesso a:
    - i) dati sensibili relativi ai pagamenti;
    - ii) risorse critiche, logiche e fisiche, quali reti, sistemi, banche dati, moduli di sicurezza, ecc;
- assicura che la "*Data minimisation*" nella progettazione, nello sviluppo e nel mantenimento dei servizi di pagamento via *Internet* sia una componente essenziale della funzionalità di base: la raccolta, il *routing*, l'elaborazione, la conservazione e/o l'archiviazione e la visualizzazione dei dati sensibili relativi ai pagamenti viene mantenuta al livello minimo assoluto.

Le misure di sicurezza per i servizi di pagamento via *Internet*:

- sono sottoposte a test per garantire la loro robustezza ed efficacia. Tutte le modifiche formano l'oggetto di un processo formale di gestione dei cambiamenti che garantisce che i cambiamenti siano correttamente ideati, sottoposti a prove, documentati e autorizzati. Sulla base dei cambiamenti effettuati e delle minacce alla sicurezza osservate, le prove vengono ripetute regolarmente e comprendono scenari di attacchi potenziali pertinenti e noti;
- sono periodicamente oggetto di verifica interna (audit) per garantire la loro robustezza ed efficacia. La frequenza e l'oggetto di tali controlli sono attinenti e proporzionali ai rischi per la sicurezza implicati. Esperti (interni o esterni) attendibili e indipendenti svolgono i controlli in questione.

Alla luce di queste considerazioni:

- l'*outsourcer* informatico (CSE) nell'ambito della propria procedura di gestione dei cambiamenti recepisce questi aspetti, inoltre vengono eseguite attività periodiche di VA e PT sia da parte di CSE che da parte di società specializzate. Con l'attività di *audit* consortile, annualmente e con il supporto di terze parti indipendenti, provvede ad effettuare una verifica sul sistema di controllo interno, andando ad effettuare anche attività di test specifiche sui sistemi di *home banking*;
- Il Consiglio di Amministrazione della Banca, sulla base delle valutazioni di rischio effettuate e degli accadimenti anomali\negativi, può approvare la richiesta di ulteriori specifici test di robustezza e sicurezza delle piattaforme tecnologiche a parti terze indipendenti e specializzate in tali interventi.
- La Banca effettua controlli periodici di terzo livello tramite la propria funzione di Internal Audit (ed eventualmente tramite la collaborazione di consulenti esterni indipendenti). In particolare viene effettuata una pianificazione degli interventi ispettivi al fine di assicurare nel tempo un'adeguata copertura delle varie applicazioni, infrastrutture e processi di gestione (incluse le componenti esternalizzate): la funzione Internal Audit fornisce proprie valutazioni sui principali rischi tecnologici identificabili e sulla complessiva gestione del rischio informatico dell'intermediario.

2.5 Tracciabilità (pto 5 Eba)

Banca Privata Leasing e l'*outsourcer* informatico CSE garantiscono che nell'ambito del servizio prestato sono inclusi meccanismi di sicurezza per la registrazione dettagliata dei dati delle operazioni e dei mandati elettronici, fra cui il numero sequenziale dell'operazione, la marcatura temporale per i dati delle operazioni, le modifiche alla parametrizzazione, e l'accesso ai dati delle operazioni e dei mandati elettronici; inoltre sono previsti dei file di registrazione (log file) che consentano la tracciabilità di aggiunte, rettifiche o cancellazioni dei dati riguardanti le transazioni o dati dei mandati elettronici sottoposti a tracciatura.

Banca Privata Leasing, per tramite del personale IT autorizzato, analizza e valuta periodicamente i dati delle transazioni e dei mandati elettronici attraverso una specifica procedura di CSE che permette l'analisi dei log (EBLS). In particolare, in CSE i logs sono trattati attraverso appositi strumenti e procedure ed accessibili solamente al personale preventivamente autorizzato ed il ciclo di addebito e di attivazione del mandato elettronico è completamente tracciato sui sistemi.

3. MISURE SPECIFICHE DI CONTROLLO E DI SICUREZZA PER I PAGAMENTI VIA INTERNET

3.1 Identificazione iniziale dei Clienti, informazioni (pto 6 Eba)

Banca Privata Leasing sottopone i propri Clienti alle procedure di adeguata verifica della clientela e monitora che la stessa abbia fornito validi documenti di identità e le relative informazioni prima che venga autorizzata ad accedere ai servizi di pagamento via *Internet*.

La Banca garantisce che le informazioni fornite al cliente contengano dettagli specifici relativi ai servizi di pagamento via *Internet*. Nell'apposita sezione del sito della Banca è presente una sezione dedicata alla sicurezza informatica (vedi *link* "SICUREZZA") che include tra l'altro:

- informazioni chiare sui requisiti del cliente in termini di apparecchiature utilizzate dall'utente, software o altri strumenti necessari (per esempio *software* antivirus, *firewall*);
- orientamenti per l'uso corretto e sicuro delle credenziali di sicurezza personalizzate;
- una descrizione passo passo della procedura con la quale il cliente inoltra e autorizza un'operazione di pagamento e/o ottiene informazioni, inclusi gli esiti di ogni azione;
- orientamenti per l'uso corretto e sicuro di tutto il *software* fornito al cliente;
- le procedure da seguire in caso di perdita o furto delle credenziali di sicurezza personalizzate, o del *software* del cliente per l'accesso o l'esecuzione delle operazioni;
- le procedure da seguire in caso di abuso riscontrato o sospetto;
- una descrizione delle responsabilità e degli oneri del prestatore di servizi di pagamento e del cliente, rispettivamente, per quanto riguarda l'uso del servizio di pagamento via *Internet*.

Banca Privata Leasing precisa al cliente che potrà bloccare una specifica operazione o lo strumento di pagamento per problemi di sicurezza, stabilendo il metodo ed i termini della comunicazione al cliente e le modalità per contattare la Banca per "sbloccare" l'operazione di pagamento via *Internet* (vedi sezione 2.3.1 del presente documento).

3.2 Autenticazione forte del cliente (pto 7 Eba)

L'inoltro dei pagamenti via *Internet*, così come l'accesso ai dati sensibili relativi ai pagamenti è protetto da un'autenticazione forte del cliente, per cui Banca Privata Leasing ed in particolare l'*outsourcer* informatico CSE, in quanto *provider* del servizio di *Home Banking*:

- prevede sistemi di *strong authentication* per l'autorizzazione di bonifici ed il rilascio o la modifica di mandati elettronici in maniera generalizzata per tutte le disposizioni di questa tipologia. A riguardo è stato predisposto:
  - un sistema di *secure call* per tutte le operazioni di pagamento;
  - un ulteriore controllo ("seconda domanda") in caso di bonifici superiori al valore di 1000 euro;
  - un sistema di controllo per i pagamenti in uscita destinati ai beneficiari di fiducia inclusi nelle "*white list*" prestabilite per quel cliente;
- prevede l'utilizzo della *strong authentication* per la modifica e l'accesso ai dati sensibili relativi ai pagamenti. A riguardo inoltre:
  - non sono previste deroghe alla suddetta autenticazione per nominativi presenti in "*white list*".

Per le operazioni con carta, tutti i prestatori di servizi di pagamento che emettono carte (*issuer*) dovrebbero supportare l'autenticazione forte del titolare della carta. Tutte le carte emesse devono essere tecnicamente pronte (registrate) per essere utilizzate con l'autenticazione forte del titolare della carta. Nel caso specifico:

- la Banca emette solamente carte di debito nazionale che non permettono di effettuare acquisti online;
- il partner che fornisce le carte di credito prevede uno specifico meccanismo di sicurezza e di controllo, tra cui il meccanismo di "Secure Code" in caso di acquisti effettuati sulla rete *Internet*.

3.3 Iscrizione (*enrolment*) e fornitura di strumenti e/o software di autenticazione al cliente (pto 8 Eba)

L'*enrolment* e la fornitura all'utente di strumenti di autenticazione e/o software per effettuare pagamenti soddisfano i seguenti requisiti:

- le relative procedure sono effettuate nei locali sicure ed affidabili della Banca;
- le relative procedure per la consegna delle credenziali di accesso sono efficaci e sicure e si concretizzano nell'invio via *mail* del codice utente e via posta tradizionale del codice *pin*: tali due codici consentono solamente l'accesso alla procedura di *home banking* informativa mentre per riuscire ad effettuare anche operazioni dispositive è necessario ulteriormente il numero telefonico indicato dall'utente;

Per le operazioni con carta di credito, la Banca si avvale dei servizi di un partner commerciale che utilizza specificatamente un sistema di *Secure Code* e durante lo *shopping online* reindirizza il cliente verso un ambiente sicuro ed affidabile.

3.4 Tentativi di accesso, sessione scaduta, validità di autenticazione (pto 9 Eba)

Banca Privata Leasing, tramite la procedura di *Home Banking* fornita dall'*outsourcer* CSE fissa il numero massimo di tentativi falliti di accesso o di autenticazione dopodiché l'accesso al servizio di pagamento via *Internet* viene permanentemente bloccato. Attualmente i tentativi massimi riservati agli utenti sono 7 (valore personalizzabile in autonomia dalla Banca), la validità della password permane per 180 giorni mentre il periodo massimo dopo il quale le sessioni dei servizi di pagamento via *Internet* inattive vengono automaticamente terminate entro il limite prestabilito dall'*outsourcer* CSE. In caso di blocco dell'utenza il processo di sblocco definito dalla Banca prevede le seguenti fasi specifiche:

- il Cliente contatta la Banca tramite i seguenti canali:
  - recandosi fisicamente in filiale – in tal caso il riconoscimento del Cliente avviene tramite il "vis-à-vis" oppure viene richiesto un documento d'identità in corso di validità. Il Cliente potrà richiedere il nuovo codice *pin* via sms sul telefono registrato sul sistema informativo in fase di sottoscrizione del contratto di conto corrente oppure direttamente tramite una busta *pin*.
  - contattando la Banca via mail all'indirizzo di posta elettronica ASSISTENZACLIENTI@BANCAPRIVATALEASING.IT. Al cliente verrà richiesto di identificarsi indicando i riferimenti del documento di identità in corso di validità censito nel sistema informativo. Una volta identificato verrà ricreato un nuovo codice *pin* inviato via sms al telefono indicato dal Cliente in fase di sottoscrizione del contratto di conto corrente *online* dispositivo.
- Nei casi di blocco dell'utenza si precisa che il codice utente non viene mai modificato mentre viene solamente ricreato un nuovo codice *pin*.
- La Banca tiene traccia delle avvenute richieste di blocco\sblocco delle utenze da parte della Clientela.

La Banca inoltre stabilisce il periodo massimo dopo il quale le sessioni dei servizi di pagamento via *Internet* inattive vengono automaticamente terminate: al momento tale limite massimo è impostato pari ad 1 minuto.

3.5 Monitoraggio delle operazioni (pto 10 Eba)

Banca Privata Leasing, per il tramite delle procedure fornite dall'*outsourcer* informatico CSE, utilizza sistemi di rilevamento e prevenzione delle frodi per individuare operazioni sospette prima che il prestatore di servizi di pagamento autorizzi da ultimo le operazioni o i mandati elettronici. Tali sistemi sono basati su regole parametrizzate come le "Black-list" dei dati relativi alle carte compromesse o rubate, il monitoraggio dei log relativi ai pagamenti e degli IBAN sospetti che vengono inviati alle funzioni competenti e automaticamente al sistema informativo per il bloccaggio.

Attraverso tali procedure vengono eseguite analisi delle transazioni e procedure di valutazione sulle stesse entro un periodo di tempo adeguato, in modo da non ritardare indebitamente l'ordine e/o l'esecuzione del servizio di pagamento in questione: se la Banca, secondo la sua politica del rischio, decide di bloccare un'operazione di pagamento identificata come potenzialmente fraudolenta, cercherà di mantenere il blocco per il più breve tempo possibile finché non saranno risolti i problemi di sicurezza.

L'entità, la complessità e l'adattabilità delle soluzioni di monitoraggio, nel rispetto della normativa in materia di protezione dei dati, sono commisurate al risultato della valutazione dei rischi ed applicando il criterio di proporzionalità citato dalla regolamentazione vigente.

Ulteriore attività di monitoraggio viene effettuata da Banca Privata Leasing nel corso dell'attività operativa quotidiana dai Responsabili delle filiali che, nell'attività di autorizzazione dei pagamenti effettuati sul canale *online*, effettuano controlli sulle possibili operazioni sospette (es: ripetizioni di operazioni di pagamento di stesso importo da parte dello stesso cliente, bonifici ripetuti verso paesi esteri, etc..).

3.6 Protezione dei dati sensibili relativi ai pagamenti (pto 11 Eba)

Tutti i dati utilizzati per identificare e autenticare i Clienti (per esempio in fase di accesso, in occasione dell'ordine dei pagamenti via *Internet* e del rilascio, della modifica o della cancellazione dei mandati elettronici), così come l'interfaccia dei Clienti (i prestatori di servizi di pagamento o il sito web degli operatori commerciali online), risultano essere adeguatamente protetti contro il furto e l'accesso o la modifica non autorizzati: in particolare l'*outsourcer* informatico CSE presidia i dati ritenuti sensibili con misure tecnologiche ritenute adeguate e concordate con la Banca.

Inoltre, l'*outsourcer* informatico CSE garantisce che, durante lo scambio di dati sensibili relativi ai pagamenti via *Internet*, sia applicata la cifratura sicura da punto a punto (*end-to-end encryption*) tra le parti comunicanti in tutta la rispettiva sessione di comunicazione, al fine di salvaguardare la riservatezza e l'integrità dei dati, utilizzando tecniche di cifratura forti e ampiamente riconosciute: in particolare la sessione di colloquio tra CSE e il Cliente Banca sono criptate con protocollo HTTPS.

4. SENSIBILIZZAZIONE, EDUCAZIONE E COMUNICAZIONE RIGUARDANTI IL CLIENTE

4.1 Educazione e comunicazione riguardanti il cliente (pto 12 Eba)

Banca Privata Leasing fornisce un canale protetto e sicuro per la comunicazione periodica con i Clienti per quanto riguarda l'uso corretto e sicuro del servizio di pagamento via *Internet*, inoltre la Banca informa i Clienti riguardo all'esistenza di questo canale e comunica che eventuali messaggi a nome della stessa forniti tramite altri mezzi, come per esempio le *e-mail*, e riguardanti l'utilizzo corretto e sicuro del servizio di pagamento via *Internet*, non sono affidabili.

Il canale protetto identificato dalla Banca si sostanzia nella funzionalità "INBOX" (all'interno dell'area riservata della procedura di *Home Banking*) e nell'indirizzo mail SICUREZZA@BANCAPRIVATALEASING.IT. Attraverso tali canali, oltre alla sezione "SICUREZZA" del sito *Internet*, la Banca informa la clientela riguardo:

- la procedura riservata ai Clienti per segnalare (presunti) pagamenti fraudolenti, incidenti sospetti o anomalie durante la sessione per i servizi di pagamento via *Internet* e/o possibili tentativi di *social engineering* (vedi sezione 2.3.1 del presente documento);
- le fasi successive, cioè in che modo la Banca risponderà al cliente (vedi sezione 2.3.1 del presente documento);
- in che modo la Banca informerà il cliente circa (potenziali) operazioni fraudolente o il loro mancato ordine, o metterà in guardia il cliente circa il verificarsi di attacchi (per esempio le *e-mail* di *phishing*).
- gli aggiornamenti riguardanti le procedure di sicurezza in relazione ai servizi di pagamento via *Internet*. Eventuali avvisi sui rischi emergenti significativi (per esempio allerta circa il *social engineering*) sono inviati alla clientela attraverso questo canale protetto.
- le indicazioni per la Clientela su come ottenere assistenza per qualsiasi domanda, reclamo, richiesta di supporto e comunicazione di anomalie o incidenti riguardanti i pagamenti via *Internet* e relativi servizi.

4.2 Comunicazioni, fissazione di limiti (pto 13 Eba)

Prima di fornire a un cliente servizi di pagamento via *Internet*, la Banca fissa i limiti applicabili a quei servizi (per esempio, un importo massimo per ogni singolo pagamento o un importo complessivo nel corso di un certo periodo di tempo) ed informa i propri Clienti di conseguenza; inoltre la Banca consente eventualmente ai Clienti di richiedere la disattivazione della funzionalità di pagamento via *Internet*, variando il profilo del cliente da dispositivo ad informativo.

Il sistema di *Home Banking* di CSE garantisce alla Banca la possibilità di definire limiti per singolo cliente e/o tipologia di operazione di pagamento eseguita da *Internet banking*: in particolare il cliente può autonomamente di abbassare i limiti, ma per qualsiasi aumento dei massimali deve essere richiesto l'intervento della Banca (attraverso richiesta scritta corredata da documento d'identità).

4.3 Accesso del cliente alle informazioni sullo stato dell'ordine e dell'esecuzione dei pagamenti (pto 14 Eba)

La Banca, tramite il servizio di *Internet Banking* prestato dall'*outsourcer* informatico CSE, garantisce ai Clienti una funzione *online* per controllare lo stato di esecuzione delle operazioni, degli ordini di pagamento e i saldi contabili aggiornati in un ambiente sicuro e affidabile.

Il sistema informativo attuale fornisce strumenti che consentono al cliente di consultare in apposita area protetta i documenti prodotti anche previa notifica tramite *alert* che comunque non include nessun dato "sensibile" del Cliente e nemmeno nessun riferimento specifico presente nel documento prodotto.